Research Paper | Education | E-ISSN No : 2454-9916 | Volume : 10 | Issue : 6 | June 2024

"CYBER CRIME CYBERSTALKING THROUGH THE CYBER LAW FORENSIC SCIENCE AND CRIMINAL INVESTIGATION"

Vyas Shivangi Anilkumar[1], Dr. Amit S. Mehta[2]

[1] Ph.D. Research Scholar, Monark University, Ahmedabad
[2] Monark University, Ahmedabad

ABSTRACT

As it is well known, the usage of the internet and mobile phones has entirely turned this world into a virtual one. In this virtual setting, Pandemic 2020 offers a fresh viewpoint on human existence. IT now serves as a crucial organ for survival. Not only has information technology expanded the sphere of development, but it has also turned into an axis for global development. People may quickly and easily access a variety of information in the virtual world. However, everything has two sides, just like a coin, and the development of information technology has sped up the growth of cybercrime everywhere.

Cyber stalking is the act of following someone using a computer or other device connected to one, which can instil terror in the victim. A relatively modern form of cybercrime is cyber stalking.

The study focuses about the meaning, nature, typology and history of cyber stalking.. This thesis compares the law relating to cyber stalking in India with different foreign countries. This thesis also discussed about the reported cases of cyber stalking from 2017-2020 as per the data of NCRB. Reason and effect of cyber staling has also been discussed in this study. Scholar suggests that there is the need of amendment of current laws specifically for the gender neutral laws and law which add the issues of international jurisdiction. Study also suggest that self-awareness is also needed for safeguard ourselves from such crimes.

Digital technology is encompassing in all walks of life, all over the world and has brought the real meaning of globalization. At the one end cyber system provides opportunities to communicate and at the other end some individuals or community exploit its power for criminal purposes. Criminals exploit the Internet and other network communications which are international in scope.

Situation is alarming; Cybercrime is an upcoming and is talk of the town in every field of the society/system. Theoretically and practically this is a new subject for researchers and is growing exponentially. Lot of work has been done and endless has to be go because the invention or up gradation of new technology leads to the technical crime
i.e. the digital or we can say the cybercrime or e-crime.

This is because every day a new technique is being developed for doing the cybercrime and many times, we are not having the proper investigating method/model/technique to tackle that newly cybercrime. Cybercrime is a criminal activity in which computers or computer networks are used as a tool, a target, or a place of criminal activity and includes everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

INTRODUCTION

Cyber crimes can be various kinds and with the advancement in science and technology, new kinds of cyber threats are coming up every other day, however, attempts have been made to categorize them so that they can be dealt with accordingly. Along with this, cyber criminals can be of various kinds as well depending upon the kind of cyber crimes they commit. Further, cyber crimes have some kind of motivation behind them such as financial gain, some vendetta, ideological motivation etc.

In Cyber Stalking, a cyber criminal uses the internet to consistently threaten somebody. This crime is often perpetrated through email, social media, and the other online medium. Cyber Stalking can even occur in conjunction with the additional ancient type of stalking, wherever the bad person harasses the victim offline. There's no unified legal approach to cyber Stalking, however, several governments have moved toward creating these practices punishable by law. Social media, blogs, image sharing sites and lots of different ordinarily used online sharing activities offer cyber Stalkers with a wealth of data that helps them arrange their harassment. It includes actions like false accusations, fraud, information destruction, threats to life and manipulation through threats of exposure. It has stalkers take the assistance of e-mails and other forms of message applications, messages announce to an online website or a discussion cluster, typically even the social media to send unwanted messages, and harass a specific person with unwanted attention. Cyber Stalking is typically cited as internet stalking, e-stalking or online stalking.

The advancement of technology has made man dependent on internet for all his needs. Internet has given man access to everything while sitting at one place. Social networking, online shopping, online studying, online jobs, every possible things that Man can think of can be done through the medium of internet.

Using the computers for our day-to-day transactions is quite common now a days. For example, we pay our life insurance premium, electricity bills, reserve flight or train or bus tickets, order book or any other product online using personal computer, smart phones, public browsing centers etc.

The number of users doing online transactions are growing rapidly ever since, because of the convenience it gives to the user to transact business without being physically present in the area where the transaction happens. Criminals committing cybercrime are also growing day-by-day with the increased number of users doing online transactions.

According to a general cyber law definition, Cyber law is a legal system that deals with the internet, computer systems, cyberspace, and all matters related to cyberspace or information technology. Cyberspace law covers a wide range of topics including aspects of contract law, privacy laws, and intellectual property laws. It directs the electronic circulation of software, information, and data security as well as electronic commerce. Edocuments are given legal recognition under cyber law. Moreover, the system provides a structure for electronic commerce transactions and electronic filing of forms. To put it simply, it is a law that deals with cyber crimes. As e-commerce has increased in popularity, it has become important to ensure there are proper regulations in place to prevent malpractices.

There are many different laws governing cyber security, largely depending on each country's territorial extent. The punishments for the same also vary according to the offence committed, ranging from fines to imprisonment. The Computer Fraud and Abuse Act of 1986 was the first cyber law that was ever to be enacted. It prohibits unauthorized access to computers and the illegal use of digital information.

Internet usage has increased, and so has cyber crimes. There are several stories of cyber crimes in the media today ranging from identity theft, cryptojacking, child pornography, cyber terrorism etc. In cyber crimes, the computer is used either as a tool or a target, or both, in order to commit unlawful conduct. In our fast-moving digital age, there has been a phenomenal surge in electronic commerce (e-commerce) and online stock trading, leading to more cyber crimes.

Ever since the creation of the Internet, people have been finding ways to conduct illegal activities using it as a tool.

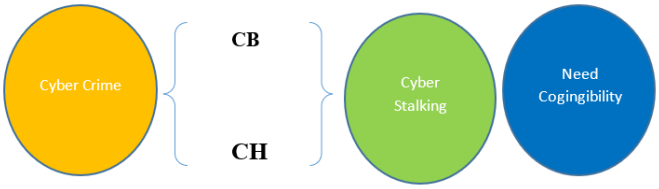
Online exploitation and abuse of girls and boys; the black cyber markets for the purchase and sale of illicit drugs and firearms; ransomware attacks and human traffickers making use of social networks to attract victims. The unprecedented scope of cybercrime - crossing borders in our homes, schools, businesses, hospitals and other vital service providers - only amplifies the threats.

Definition of cyber crime

Although it is universally agreed that cybercrime exists, there is no universal definition of what it means but still we can say that

Cyber crime is a criminal activity that uses a computer to target the computer or it maybe defined as a crime where a computer is the object of the crime and is used as a tool to commit an offense.

Cybercrimes fall under State subjects as per the Seventh Schedule of the Constitution of India.



Meaning of Cyber Crime:

Cybercrime is an offence involving a computer, computer network, electronics, and electronic communication, as well as information methods, in which the computer is utilised as a tool, a target, or both.

"Cyber Crime" can be defined as any criminal conduct involving electronic communications or information systems, including any device or the Internet, or both or both of them. In brief, "Cyber Crime" refers to offences or crimes committed via electronic communications or information technologies. The term cyber refers to the computermodeled information space in which various items or information in the form of symbols and images exist. As a result, the place where computer programs operate and data processing takes place.

The term "cyber" comes from the phrase "cybernetics," which means science of communication and control over machines and people. Cyberspace is a new horizon intended for information and communication between human being from all over the world that is controlled by machines. As a result, cybercrime refers to crimes performed in cyberspace involving equipment or devices, as well as crimes involving cyber technology. Information technology and internet commerce are frequently utilised to aid or perpetrate criminal activity. Hacking, terrorism, fraud, unlawful gambling, cyber stalking, cyber theft, forgery, and cyber pornography are all examples of cyber crime in a broader sense.

In any statute, the term cybercrime is not defined. Any unauthorized/ unlawful act, commissioned with the use of a computer or computer network or communication device, to commit or facilitate the crime is called cyber-crime.

Impact of Cyber crime

Cyber Crime has a great impact on the people as people are facing loses socially, economically as well as emotionally.

The people are suffering economically as the cyber criminals by utilising their information hack the peoples bank account or commit fraud and transferred the money from their bank accounts in different ways. There is social impact of the cyber crime as the criminals uses the personal information of the people for committing different crime as cyber pornography, leak confidential information, cyber bullying and other crime committed due to which the society is affecting at large. It also affected the people emotionally and, in some cases, people blamed themselves for the loss occurred to them.

Child Pornography / Child Sexually Abusive Material (CSAM)	CSAM refers to content having an image of sexual in nature, of a child, abused or sexually exploited. Section 67 (B) of the Information Technology Act states that publishing/transmitting any material, in electronic form, portraying children in sexually explicit acts, is a punishable cyber-crime.
Cyber Bullying	A bullying or a form of harassment perpetrated through electronic media or communication devices such as laptop, computer, mobile phone etc.
Cyber Stalking	• It is the use of electronic media by a person to track a person or tries to communicate/ contact another person to impose personal interaction continually despite the reluctance and disinterest by such person; • To monitor the email, internet or any other form of electronic communication of the other person and thereby committing an offence of stalking.
Online Job Fraud	Wherein a person who is in need of a job is duped for money or defrauded by giving him/her fake promises to employment with higher wages through electronic communication.
Online Sextortion	When someone threatens to circulate or publish any sensitive/ private material/ images/ content using electronic medium if the other person rejects or denies providing images, favors of sexual nature or money.
Vishing	Fraudsters try to obtain personal information like bank account password, customer ID, ATM PIN, OTP, credit card CVV etc. over a phone call.
Phishing	It is a type of fraud that involves stealing of personal information of a person such as a bank's customer ID, Credit Card/ Debit Card number, CVV number, etc. through electronic channels that seem to be from a genuine source.
Ransomware	• A computer malware that encrypts the storage media and files on electronic devices like mobile phones, laptops, desktops, etc., by taking control over the data/ information as a hostage.
	• The aggrieved are demanded ransom to get his information/ data decrypted or else they are threatened to even sell the data/ information on the dark web.

Historical Background

Over the past decade, cybercrime has become a big business — a $1.5T industry with an entire ecosystem of criminal organizations run like legitimate organizations. Some even offer technical leadership, step-by-step instructions, and robust customer service via ransomware-as-a-service (RaaS), and the most brazen threat actors have even taken out pop-up ads selling their products. Factor in nation-state actors, individual hackers targeting specific organizations, and third-party hacks that hit multiple businesses at once, and you have a target-rich threat environment for IT and security teams to defend against.

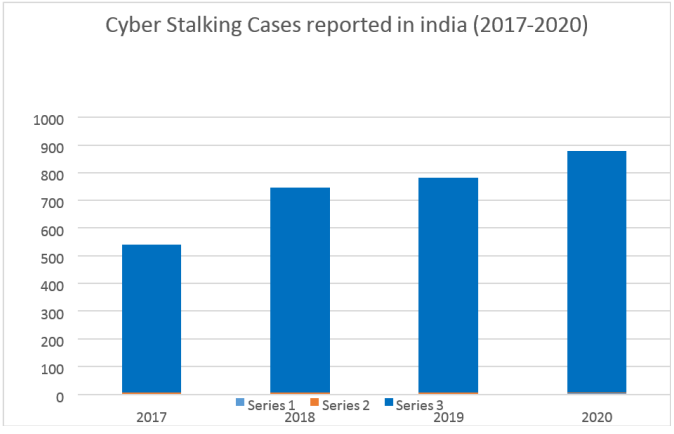
Yet, while the cybercrime industry has exploded in the past ten years, the truth is that cybercrime is not a new kind of threat. In fact, it goes back not just a decades but centuries.

Technically, the first cyber attack happened in France well before the internet was even invented, in 1834. Attackers stole financial market information by accessing the French telegraph system. Still, cybercrime didn't really find its footing until the late 20th century. Spurred on by the digital revolution, cybercriminals became early adopters of technology, using their head start and their smarts to engineer new, devious ways to part people and organizations from their data and dollars. From that moment on, cybercrime has grown exponentially, marked by an evolution of tactics, techniques, and procedures (TTPs) — all implemented for malicious gain.

Now, cybercrime has expanded into its own ecosystem, full of leak sites, "as-aservice" models, lucrative attack vectors such as business email compromise (BEC), and an expanding global footprint that costs organizations more and more every year.

Reported cases and disposal of cyber stalking:

In India, the National Crime Records Bureau (NCRB) included statistics on cyber stalking/cyber bullying against women/children for the first time in its 2017 report, finding a total of 542 incidents reported under this heading in that year.177Furthermore, according to a Microsoft report on 'Global Youth Online Behaviour' performed in 2018, India is third on the list of countries where more than half of children (53 percent) have been harassed online. India is ranked third in the world, behind China (70 percent) and Singapore (58 percent).178 In comparison to the rest of India, Maharashtra had the largest number of cyber stalking and bullying occurrences against women and children in 2020, with over 388 cases reported to police. With 145 cases, Andhra Pradesh came in second. In total, 872 occurrences of such offences were reported in the country in the same year.179 Section 354D of the Indian Penal Code covered this type of offence. The above-referred incidents of India have been enumerated in details under the figure 1, 2, 3, 4, and 5.



Police Disposal of Cyber Stalking Cases from 2017-2020:

S.No.	Nature	2017	2018	2019	2020
1	Cases Pending Investigations from Previous Year	82	331	559	742
2	Cases Reported during the year	542	739	777	872
3	Cases Reopened for Investigation	0	4	0	0
4	Total Cases for Investigation (Col.3+Col.4 +Col.5)	624	1074	1336	1614
5	Cases Not Investigated Under 157_1_b CRPC	0	0	0	0
6	Cases Transferred to other State or Agency	1	1	3	1
7	Cases Withdrawn by the Govt during investigation	0	0	0	0
8	Cases Ended as FR Non Cognizable	0	0	0	0
9	Cases Ended as Final Report False	12	11	28	13
10	Cases Ended as Mistake of Fact or of Law or Civil Dispute	8	15	12	11
11	Cases True but Insufficient Evidence or Untraced or No Clue	36	81	78	88
12	Cases Abated during Investigation	1	0	6	2
13	Total (Col.8+ Col.9+ Col.10+ Col.11+ Col.12)	57	107	124	114
14	Cases Chargesheeted Out of Cases from Previous Year	35	89	149	167
15	Cases Chargesheeted Out of Cases during the Year	198	301	317	271
16	Cases Chargesheeted (Col.14+ Col.15)	233	390	466	438
17	Total Cases Disposed Off by Police (Col.5+ Col.6+Col.13+ Col.16)	291	498	593	553
18	Cases Quashed at Investigation Stage	0	1	6	0
19	Cases Stayed at Investigation Stage	1	0	0	0
20	Pending Investigation at End of the Year (Col.4- Col.7- Col.17	333	575	737	1061
21	Charge-Sheeting Rate (Col.16/ Col.17) *100	80.1	78.3	78.6	79.2
22	Pendency Percentage (Col.20 / Col.4) *100	53.4	53.5	55.2	65.7

CONCLUSION

The Information Technology Act of 2000 dand the Indian Penal Code of 1860 do not specifically address the subject of cyber stalking and the defamatory or threatening statements made by the stalker while stalking the victim through SMS, phone calls, e-mails, or blogging under the victim's name. Some of the provisions of the above-mentioned Acts allow for the punishment of the offender. There is no specific clause that deals with this offence. This crime is fairly simple to commit, but the consequences are quite long-lasting. It can harm the victim's mental and physical well-being. The penalty provided under current provisions should be enhanced while keeping the victim's well-being in mind.

The best place to lodge concerns is via an online help desk or cyber cell. To comply with Rule 2(b) of Chapter II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, websites must remove reported material within 24 hours. Victims have the option of contacting CERT-IN (Indian Computer Emergency Response Team), a nodal body designated under Section 70B of the IT Act, in addition to the police. The victim may also submit a complaint via the National Cyber Crime Reporting Portal.

The most effective way involves the individual creating their own rules, such as requiring a complex password with both letters and digits. Equally important is limiting the amount of personally identifiable information shared about oneself on social media. The Information Technology Act has to be revised to make law enforcement easier, and the scope of existing laws should be expanded to encompass extraterritorial jurisdiction.

REFERENCES

1. Indian Legislation on Cyber Crime (S. R. Sharma)Indian Evidence Act, 1872
2. Cyber Frauds, Cybercrimes & Law In India (Pavan Duggal)
3. Cyber Crime Investigations (Anthony Reyes)
4. Cyber Crime and Cyber Laws in India (Abhishek Sharma P., Dr. Ayan Das Gupta)